Arithmetic of Squares (整数論)

AUTHOR(S):

UCHIYAMA, SABURO

CITATION:

UCHIYAMA, SABURO. Arithmetic of Squares (整数論). 数理解析研究所講究録 1977, 294: 95-99

ISSUE DATE:

1977-04

URL:

http://hdl.handle.net/2433/106202

数理解析研究所講究録
294 巻 1977 年 95-99

ARITHMETIC OF SQUARES

Saburô UCHIYAMA

Department of Mathematics, Okayama University

We shall discuss two, mutually independent problems concerning some arithmetic properties of squares; the one being posed by P. Erdös (1960) and the other by S. Hitotumatu (1976). This article is a brief exposition of the results obtained: detailed accounts thereof have already been, or will soon be, published elsewhere.

I. *The Number of Squares in an Arithmetic Progression*

Let a and b be arbitrary integers with $a > 0$ and $b \geq 0$. For any real number $x > 0$ we denote by $A(x; a, b)$ the number of those integers $an + b$ $(0 \leq n \leq x)$ which are the square of an integer. P. Erdös has conjectured that to every $\varepsilon > 0$ there corresponds a number $x_0 = x_0(\varepsilon)$ such that

$$A(x; a, b) < \varepsilon x \quad \text{for} \quad x > x_0. \tag{1.1}$$

A conjecture of W. Rudin states that there is an absolute constant $c > 0$ such that

$$A(x; a, b) < c\sqrt{x} \quad \text{for} \quad x \geq 1. \tag{1.2}$$

Recently, E. Szemerédi (1974) has given a very short (but by no means elementary) proof of (1.1) by noticing that there are no four squares that form an arithmetic progression, an observation due to L. Euler, and by appealing to his own result to the effect that every infinite sequence of non-negative integers that has positive upper density contains an arithmetic progression of four (or more) elements.

We shall give another simple and elementary proof of (1.1).

There is no loss in generality in assuming that $a > b$. Every non-negative integer belongs to one and only one arithmetic progression of the form $an + b$ $(n \geq 0)$, where a is fixed and $0 \leq b < a$. Hence we have

$$\sum_{b=0}^{a-1} A(x; a, b) = [\sqrt{ax + a - 1}] + 1 \qquad (x > 0),$$

where $[t]$ denotes the greatest integer not exceeding the real number t; this implies that

$$A(x; a, b) \leq \sqrt{ax + a - 1} + 1 \qquad (x > 0)$$

for any a and b with $a > b \geq 0$, since we have always $A(x; a, b) > 0$. This clearly proves (1.1).

We note that neither the sophisticated proof of Szemerédi's nor our straightforward proof just given does not establish the uniformity in a and b, if true, of the inequality (1.1).

It is possible to find an asymptotic evaluation for $A(x; a, b)$ from which follows an inequality nearly as sharp as (1.2). Now, given a and b, we write

$$(a, b) = d = e^2 f, \quad a = da_o \quad \text{and} \quad b = db_o, \quad (a_o, b_o) = 1,$$

where e^2 is the largest square factor of d, so that f is a squarefree integer. We have for $x > 0$

$$\left| A(x; a, b) - \frac{N(a, b)}{a} (\sqrt{ax + b} - \sqrt{b}) \right| \leq \frac{N(a, b)}{e},$$

where $N(a, b)$ denotes the number of incongruent solutions $u \pmod a$ of the congruence $u^2 \equiv b \pmod a$. Since

$$N(a, b) = eN(a_o, fb_o)$$

and since

$$N(a_o, fb_o) = O(a_o^{\varepsilon}) \quad \text{for any fixed } \varepsilon > 0,$$

where the O-constant may depend on ε, it follows from this that

$$A(x; a, b) = O\left(a_o^{\varepsilon}\left(\sqrt{\frac{x}{a_o}} + 1\right)\right) \qquad (x > 0); \tag{1.3}$$

this inequality is in general stronger than (1.2) for large values of x but is weaker than (1.2) for small values of x.

Professor E. Bombieri remarks that an application of the sieve of H. L. Montgomery yields the result

$$A(x; a, b) = O\left(\left(\frac{a}{\phi(a)}\right)^2 \sqrt{x}\right) = O((\log\log 3a)^2\sqrt{x})$$

for $x > 1$, the O-constants implied being absolute; this result is better than (1.3) for smaller values of x.

References

P. Erdös: Quelques problèmes de la théorie des nombres. Monographies de l'Enseignement Mathématique No. 6 (Non dated). Problème 16, p. 91.

E. Szemerédi: The number of squares in an arithmetic progression. Studia Sci. Math. Hungar. 9 (1974), 417.

S. Uchiyama: On the number of squares in an arithmetic progression. Proc. Japan Acad. 52 (1976), 431-433.

II. *A Five-Square Theorem*

It is clear that for every even integer $2n > 0$ there is a natural number s such that $2n$ is representable in the form

$$2n = \sum_{i=1}^{s} x_i^2 \quad \text{with the condition} \quad \sum_{i=1}^{s} x_i = 0, \tag{2.1}$$

where the x_i $(1 \leq i \leq s)$ are rational integers. We denote

by $s(2n)$ for a given $2n$ the smallest possible value of such s. We have evidently $2 \leq s(2n) \leq 8$ for all $2n > 0$.

It is proved that we have

(2.2) $$s(2n) \leq 5 \quad \text{for all} \quad 2n > 0$$

with the equality exclusively for the integers $2n$ of the form

$$4^k(32\ell + 28) \qquad (k \geq 0,\ \ell \geq 0).$$

The problem of determining the value of

$$\max_{n \geq 1} s(2n)$$

has been (orally) communicated to the writer by Professor S. Hitotumatu of RIMS, Kyoto University, who was led to this problem in the course of his study of 'translatable complete ℓ-th power configuration.' Our result (2.2) gives a satisfactory solution for the problem proposed.

We note that the result (2.2) is a particular case of a general theorem due to G. Pall; however, our treatment is much more direct and more elementary (simpler, at least) than Pall's.

Our proof of (2.2) depends on the following

Lemma. Let m be a positive integer. The integer m can be represented in the form

$$m = x^2 + y^2 + z^2$$

with some integers x, y, z, if and only if m is not of the form

$$4^k(8\ell + 7) \qquad (k \geq 0,\ \ell \geq 0);$$

the integer m can be represented in the form

$$m = x^2 + y^2 + 2z^2$$

with some integers x, y, z, if and only if m is not of the form

$$4^k(16\ell + 14) \qquad (k \geq 0,\ \ell \geq 0).$$

The first part of the lemma is a well-known result, and the second part is a direct consequence of the first part.

No representations of the type (2.1) are possible for odd integers. An analogue to (2.1) for the representation of an odd integer $2n + 1 > 0$ will be

$$2n + 1 = \sum_{i=1}^{s} x_i^2 \qquad \text{with} \qquad \sum_{i=1}^{s} x_i = 1,$$

where the x_i are again rational integers. If we denote by $s(2n+1)$ for a given $2n+1$ the smallest possible value of s in the above representation, then it can be shown that we have

$$s(2n+1) \leq 4 \qquad \text{for all} \quad 2n+1 > 0.$$

This result also is a special case of Pall's.

References

G. Pall: Simultaneous quadratic and linear representation. Quart. J. Math. (Oxford) 2 (1931), 136-141.

S. Uchiyama: A five-square theorem. Publ. RIMS, Kyoto Univ. 13 (1977), no. 1, to appear.